UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/604,174	06/27/2000	John L. Manferdelli	MSFT-0188/154574	4724

41505 7590 01/03/2007

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/604,174	MANFERDELLI ET AL.	
	Examiner	Art Unit	
	Christopher J. Brown	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32,34-46 and 49-73* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-32, 34-46, 49-73* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The Request for Continued Examination has been accepted and entered.

Response to Arguments

Applicant's arguments filed 10/11/06 with respect to the USC 112 rejection of claims 1-31 and 60 have been fully considered but they are not persuasive. With respect to the USC 112 Applicant argues that the amendments made more clearly define the invention. However in each case the application of encryption protocols still accesses a cryptographic key. Page 7 lines 20-26 of the instant specification state the problem best. The black box performs cryptographic functions, "preferably equipped with one or more cryptographic keys".

Applicant's argument with respect to the USC 102 rejection by Granger US 6,643,775 has been fully considered but is not persuasive.

The applicant argues that Granger does not suggest "said computer program does not require access to said cryptographic key", and rather that Granger does teach requiring access to said cryptographic key.

The examiner argues that in light of the specification on the current invention, and claims, Granger teaches a system that performs in a similar manner. Although Granger teaches that the encryption layer uses a key, Granger states in Col 7 lines 7-20, that the encryption layer code which performs the encryption and decryption of userdata may be

written in a pseudocode, thus creating a new program that does not require said key. Also Granger teaches that pseudocode may be used in conjunction with obfuscation to rewrite the encryption algorithm (Col 9 lines 25-47).

The examiner suggests removing the word "can" in claim 1. The word "can" suggests that the invention may do a thing, but does not have to do it.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 22, 32, and 45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 22, 32, and 45 state that a computer program applies a cryptographic key to a first data. These claims also state the computer program does not require access to the cryptographic key. It is clear from the instant specification that the applicant intends to essentially emulate a key to apply a key without "requiring access to said cryptographic key". However, the computer program still needs to analyze said key before it emulates it in code, (Specification page 19 lines 3-22) and needs access to the key in order to analyze it. The invention states that a black box to perform one or more cryptographic functions is equipped with one or more cryptographic keys (Specification page 7 lines 7-

20). Furthermore every claim must be interpreted with the broadest reasonable interpretation.

Claims 1, and 22 state applying a key without access to a key, which is indefinite using the broadest reasonable interpretation. The explanation from the specification is not also stated in claims 1, or 22. Appropriate correction is required.

Dependent claims based on the rejected base independent claims 1, 22, 32, or 45 are also rejected.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claim 1-4, 6-8, 12, 14, 15, 16, 21, 22, 26, 31, 32, 33, 34, 39, 44, 45, 47-50, 53, 55, 56, 57, 62, 65, 66, 69, are rejected under 35 U.S.C. 102(e) as being anticipated by Granger US 6,643,775.

As per claims 1, 21, 22, and 31 Granger teaches using a program to generate and apply a key to first data, (Col 6 lines 25-40). Granger teaches taking a set of actions (encrypting) using pseudocode so that access to the key is not necessary, (Col 6 lines 55-60, Col 7 lines 8-20). Granger teaches performing a diversionary set of actions while performing cryptographic actions as a form of obfuscation, (Col 12 lines 43-60).

As per clams 2, and 3, Granger teaches the cryptography may be public key cryptography, (Col 10 lines 20-27).

As per claims 4, 49, and 65 Granger teaches receiving a second data that relates to the computing device upon which the program runs, where the first set of instructions is based on said second data, (Col 6 lines 15-27).

As per claim 6, Granger teaches the received data is necessary for encryption/decryption, (Col 6 lines 25-27).

As per claims 7, 50, and 66 Granger teaches using a random number in the executable instructions, (Col 12 line 55).

As per claims 8 Granger teaches performing a diversionary set of actions while performing cryptographic actions as a form of obfuscation, (Col 12 lines 43-60).

As per claims 12, and 53 Granger teaches reorganizing code in a computer program, (Col 7 lines 63-67).

As per claims 14, 16, 26, 39, 55, and 57 Granger teaches that instructions are encrypted, and decrypted when needed, (Col 7 lines 8-20).

As per claims 15, 56, and 69 Granger teaches the program is written in source and compiled, (Col 7 lines 53-59).

As per claims 32, and 44 Granger teaches using a program to execute a first action, (Col 6 lines 33-40). Granger teaches a sub-action, (Col 12 lines 43-47). Granger teaches a second action that is different from the first action, (Col 12 lines 56-61).

As per claims 33, and 34 Granger teaches using a key to decrypt first data, (Col 6 lines 25-30).

As per claim 45, 47, 48, and 62 Granger teaches using a program to generate and apply a key to first data, (Col 6 lines 25-40). Granger teaches converting first program into a second program using pseudocode so to perform the same function, without access to said key (Col 6 lines 55-60, Col 7 lines 8-20).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5, 17, 18 , 24, 58, and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Maytal US 6,715,079.

As per claims 5, and 24, Granger teaches a program, but does not teach that the program is based on data that identifies the CPU.

Maytal teaches receiving a program with data customizing the program so that it only works on the Computer with the correct CPUID, (Col 10 lines 16-53 Fig 12).

It would have been obvious to one of ordinary skill in the art to modify the program of Granger with the data of Maytal because the customized program will prevent illegal copying and use without the appropriate CPUID.

As per claims 17, 18, 58 and 59, Granger does not disclose downloading a program over the Internet.

Maytal teaches CPU's submitting data to request a customized computer program may be downloaded to the computer over the Internet, (Col 10 lines 25-35). It would have been obvious to one of ordinary skill in the art to modify the program of Granger with the delivery of Maytal because distribution over the Internet is cheaper and faster than other delivery methods.

Claims 9, 20, and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Matsui US 2002/0178412.

As per claims 9, 20, and 61 Granger does not teach retrieving instructions from a database.

Matsui teaches retrieving instructions from a database [047].

It would have been obvious to one obvious to one of ordinary skill in the art to modify Granger with the database of Matsui because it can be retrievable at any terminal with network access.

Claims 13, 28, 29, 35, 41, 42, 54, and 64, are rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Moskowitz 6,958,162.

As per claims 13, 28, 29, 35, 41, 42, 54, and 64, Granger does not teach delimiting or hashing.

Moskowitz teaches delimiting a file and hashing it (Col 8 lines 23-40). Moskowitz teaches the hash may be used for authentication, (Col 8 lines 35-40). It would have been obvious to use the properties of Moskowitz with the system of Granger because Moskowitz increases uniqueness and security.

Claims 19, and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Maytal US 6,715,079 in view of Frasier US 5,758,293

As per claims 19, and 60 Granger does not disclose downloading a program over the Internet.

Maytal teaches CPU's submitting data to request a customized computer program may be downloaded to the computer over the Internet, (Col 10 lines 25-35). It would have been obvious to one of ordinary skill in the art to modify the program of Granger with the

delivery of Maytal because distribution over the Internet is cheaper and faster than other delivery methods. Maytal does not specify the timetable for downloading.

Frasier teaches that data is downloaded contemporaneously with a request for said data, (Col 1 lines 17-23). It would have been obvious to use the contemporaneous download of Frasier with Maytal because it allows for the quick transfer of data.

Claims 10, 23, 36, 37, 51, and 68 and 30-34, 36, 37, 43-48, 50, 51, 53, 56, 57 62, and 66-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Aucsmith US 5,892,899.

As per claims 10, 23, 36, 37, 51 and 68 Granger teaches integral diversionary computer actions.

Aucsmith teaches extra obfuscation subprograms that are diversionary in nature, and unrelated to key and first data (Col 6 lines 23-27). It would have been obvious to one of ordinary skill in the art to add the obfuscation subprograms the original program of Granger so that the original program's obfuscation level is raised.

Claims 30, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Yarom US 5,949,573.

As per claims 30, and 43, Granger does not teach moving the program to a random memory location.

Yarom teaches moving the memory location of the program (Col 3 lines 60-67). It would have been obvious to use the random memory moving of Yarom with the system of Granger because Yarom's random memory method prevents attackers from knowing where the code resides, (Col 4 lines 1-4).

Claim 46 is rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Carver US 5,850,554

As per claim 46, Granger does not teach inline code.

Carver teaches use of inline code with compliers and programs, (Col 12 lines 34-40). It would have been obvious to use the inline code of Carver with the system of Granger because it allows more efficient modification to the code.

Claims 11, 25, 38, 52, 63, 67 and 71-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Barton US 5,912,972

As per claims 11, 25, 38, 52, and 63, 67, and 71-73 Granger teaches using a program to generate and apply a key to first data, (Col 6 lines 25-40). Granger teaches taking a set of actions (encrypting) using pseudocode so that access to the key is not necessary, (Col 6 lines 55-60, Col 7 lines 8-20). Granger teaches performing a diversionary set of actions while performing cryptographic actions as a form of obfuscation, (Col 12 lines 43-60). Granger teaches creating computer executable instructions, but does not teach error detection.

Barton teaches error detection and correction, (Col 9 lines 9-16).

It would have been obvious to one of ordinary skill in the art to add the error correction to n the system of Granger because the error correction would maintain the data and prevent errors.

Claims 27, 40, and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Granger US 6,643,775 in view of Aucsmith US 5,892,899 in view of Johnson US 5,682,428

As per claims 27, 40, and 70 The prior Granger-Aucsmith combination does not teach decrypting a program using it and then re-encrypting it.

Johnson teaches decrypting a file, manipulating it and then re-encrypting it, (Col 27 lines 32-37). It would have been obvious to one of ordinary skill in the art to add the encryption of Johnson to the Granger-Aucsmith combination to increase security.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown

12/22/06

KAMBIZ ZAND
PRIMARY EXAMINER